Seguridad Informática
Conceptos generales.

Luis Alonso Romero
Catedrático de Ciencia de la Computación e Inteligencia Artificial.
Universidad de Salamanca

Bibliografía

- Seguridad y protección de la Información.- Morant, Ribagorda, Sancho.- Centro de Estudios Ramón Areces, 1994
- Computer Networks, 3rd Ed.- Tanenbaum.- Prentice Hall 1996
- Comunicaciones y Redes de Computadores, 5ª Ed .- Stallings.-. Prentice Hall 1997
- Computer Security Basics.- Russell, Gangemi.- O'Reilly
- Seguridad y protección de la información. Universidad Jaime I.- http://spisa.act.uji.es/SPI
- Network and Internet Network Security. Principles and Practice. W. Stallings. Prentice Hall 1995
- Secure Computers and Networks. E. Fish; G.B. White. CRC Press LLC, 2000

Contenidos

- Definiciones.
- Criterios de seguridad.
- Tipos de ataques.
- Medidas y políticas de seguridad.
- Principios fundamentales.
- Seguridad en Sistemas Operativos.
- Seguridad en Bases de Datos.
- Seguridad en Redes.

Definiciones

- Definiciones del DRAE, 22 edición (2001):
  - Seguridad:
    - Cualidad de seguro.
    - (Mecanismo).- Que asegura un buen funcionamiento, precaviendo que éste falle, se frustre o se **violente.**
  - Información:
    - Comunicación o adquisición de conocimiento que permiten ampliar o precisar los que se poseen sobre una materia determinada.
    - *El conocimiento es lo que permite al soberano saber y al buen general intuir, esperar y anticiparse. (Sun Tse, siglo V a.C)*
    - *Nam et ispa scientia potestas est (Bacon)*
  - Protección:
    - Resguardar a una persona, animal o cosa de un perjuicio o peligro.

Seguridad en las TIC

- En los últimos tiempos se han realizado grandes avances en las tecnologías de la información y las comunicaciones (TIC).
- Los sistemas informáticos se han introducido de forma generalizada en el comercio, banca, industria, administración, defensa, investigación, ...
- La aparición y expansión de Internet, juntamente con los sistemas informáticos, han hecho posible la realización de tareas impensables hace unos pocos años: transacciones bancarias, resolución de problemas complejos, control, docencia, comercio electrónico, B2B, ...
- Pero, a medida que los sistemas de información son más complejos, han puesto de manifiesto una mayor cantidad de puntos vulnerables:
  - El número de posibles atacantes crece muy rápidamente.
  - Los medios disponibles para efectuar ataques siguen una evolución tan rápida como los propios sistemas.
  - La generalización de Internet hace que los ataques puedan provenir de cualquier lugar.

¿Qué hay que proteger?

- Es evidente la necesidad de proteger la información.
- Pero es muy difícil concretar qué es lo que hay que proteger, dado que el concepto de información es, en sí mismo, poco claro.
- Se choca también con el derecho a la intimidad:
  - Los gobiernos, y la empresas, necesitan multitud de datos de los ciudadanos, o clientes, para poder hacer planificaciones, estrategias de ventas, promover leyes, censos, tratamientos médicos, etc.
  - Algunas de esas informaciones pueden ser manipuladas o utilizadas con fines distintos a los originales, o ser empleadas por organizaciones a las que no se les entregaron en su momento.

Sistemas informáticos

- Un sistema informático es el conjunto de elementos hardware, software, datos y personas que permiten el almacenamiento, procesamiento y transmisión de información.
- Todos los elementos de un sistema informático son vulnerables:
  - Hardware : aislamiento de los CPD, sistemas contra incendios, SAIs, etc.
  - Software: bombas lógicas, caballos de Troya, gusanos, virus, ..
  - Personas que trabajan en la administración de los CPD, en la gestión de los sistemas de comunicaciones, etc.
  - Datos: son los ataques más sencillos de practicar y, por lo tanto, donde más se necesita la aplicación de políticas de seguridad.

Criterios de seguridad

- El Information Technology Security Evaluation Criteria (ITSEC) define los siguientes criterios de seguridad:
  - **Secreto o confidencialidad**: la información debe estar disponible solamente para aquellos usuarios autorizados a usarla.
  - **Integridad**: la información no se puede falsear. Los datos recibidos (o recuperados) son los mismos que fueron enviados (o almacenados), etc.
  - **Accesibilidad o disponibilidad**: ¿quién y cuándo puede acceder a la información?
    - La falta de accesibilidad produce una **denegación de servicio**, que es uno de los ataques más frecuentes en Internet.
  - **Autenticidad**: asegurar el origen y el destino de la información.
  - **No repudio**: cualquier entidad que envía o recibe datos no puede alegar desconocer el hecho.
    - Los dos criterios anteriores son especialmente importantes en el entorno bancario y de comercio electrónico.

Más criterios de seguridad relacionados.

- **Consistencia**: asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados.
- **Aislamiento**: impedir que personas no autorizadas entren en el sistema.
- **Auditoría**: capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema y quién y cuándo las han llevado a cabo.
- **Prevención**: los usuarios deben saber que sus actividades quedan registradas.
- **Información**: posibilidad de detectar comportamientos sospechosos.
- .....

Aspectos negativos

- **Vulnerabilidad**: punto o aspecto del sistema que es susceptible de ser atacado. Equivale al conjunto de debilidades del sistema.
- **Amenazas o ataques** (*Threats*): Posible peligro del sistema. Pueden provenir de personas (*hackers*, *crackers*), de programas, de sucesos naturales. Equivalen a los factores que se aprovechan de las debilidades del sistema.
- **Contramedidas**: técnicas de protección del sistema contra las amenazas.
  - La seguridad informática se encarga de identificar las vulnerabilidades del sistema y establecer las contramedidas necesarias para intentar evitarlas.
  - **Axioma de seguridad**: No existe ningún sistema absolutamente seguro.

Tipos de vulnerabilidad

- Algunos tipos de vulnerabilidad pueden ser:
  - **Natural**: desastres naturales o ambientales.
  - **Física**:
    - acceso físico a los equipos informáticos,
    - a los medios de transmisión (cables, ondas, ...), etc.
  - **Lógica**: programas o algoritmos que puedan alterar el almacenamiento, acceso, transmisión, etc.
  - Humana: Las personas que administran y utilizan el sistema constituyen la mayor vulnerabilidad del sistema.
    - Toda la seguridad del sistema descansa sobre el administrador, o administradores.
    - Los usuarios también suponen un gran riesgo.

Tipos de ataques

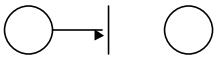
- Sistema que proporciona información: flujo de información fuente-destino.

Situación normal:

Flujo normal

Tipos de ataques II

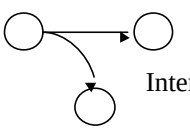
– *1.- Interrupción*: Destruye información o la inutiliza: Ataca la accesibilidad o disponibilidad



Interrupción

Destruir algún dispositivo.
Saturar la capacidad del procesador,

– *2.- Intercepción*: Una parte no autorizada gana el acceso a un bien. Ataca la confidencialidad.



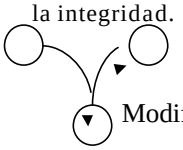
Intercepción

intruso

Escuchas en línea de datos.
Copias no autorizadas, ...

Tipos de ataques III

– *3.- Modificación*: Una parte no autorizada modifica el bien. Ataque a la integridad.

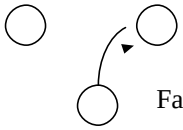


Modificación

intruso

Cambiar contenidos de bases de datos, cambiar líneas de un programa, datos de una transferencia, etc.., ...

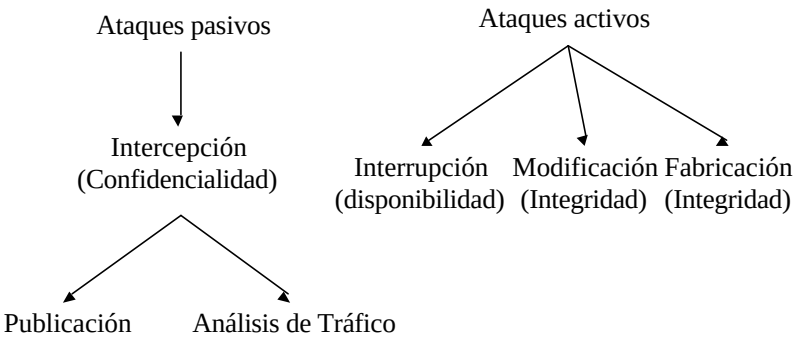
– *4.- Fabricación*: Falsificar la información: Ataca la autenticidad.



Fabricación

Añadir campos y registros en una base de datos, añadir líneas de un programa (virus), etc.., ...

Tipos de ataques III



Medidas de seguridad

- Las medidas de seguridad se suelen clasificar en cuatro niveles:
  - **Físico**: impedir el acceso físico a los equipos informáticos, a los medios de transmisión (cables de argón, por ejemplo), etc.
    - Vigilancia, sistemas de contingencia, recuperación, ...
  - **Lógico**: establecer programas o algoritmos que protejan el almacenamiento, acceso, transmisión, etc.
    - Contraseñas, Criptografía, cortafuegos, ...
  - **Administrativo**: en caso de que se haya producido una violación de seguridad, ¿cómo se delimitan las responsabilidades?
    - Publicación de la política de seguridad.
  - **Legal**: ¿qué se hace en caso de ataques, violaciones, que hayan sido comprobadas?
    - Normalmente, transcienden el ámbito empresarial y son fijadas por los gobiernos o instituciones internacionales.

Política de seguridad

- La política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas de información y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.
  - Se plasma en una serie de normas, reglamentos y protocolos a seguir donde se definen las distintas medidas a tomar para proteger la seguridad del sistemas, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar el funcionamiento correcto.
    - ¿Qué necesitamos proteger?
    - ¿De qué necesitamos protegerlo?
    - ¿Cómo lo vamos a proteger?
    - .....

Análisis y gestión de riesgos

- Los objetivos de la seguridad de un sistema de información son mantener la información:
  - Confidencial
  - Integra
  - Disponible
- Una **violación de la seguridad** es cualquier suceso que comprometa estos objetivos.
- El **Análisis y la Gestión de riesgos** es un método formal para investigar los riesgos de un sistema de información y recomendar las medidas apropiadas para controlarlos.

Análisis y gestión de riesgos II

- En el análisis de riesgos hay tres costes fundamentales:
  - C_r : Valor de los recursos y la información a proteger.
  - C_a : Coste de los medios necesarios para romper las medidas de seguridad implantadas en el sistema.
  - C_s : Coste de las medidas de seguridad.
- Es evidente que se debería cumplir que:
  - $C_a > C_r > C_s$
  - Es decir, el coste de romper las medidas de seguridad es mayor que el de los posibles beneficios obtenidos.
  - El coste de las medidas de seguridad es menor que el de los recursos protegidos.
  - De los tres sumandos es C_r el más difícil de evaluar.
  - C_r = Valor intrínseco (hardware, software, datos, patentes, ...)
    + Costes derivados de su pérdida, intercepción o modificación (reposición, repetición de experimentos, recuperación, ...)

Principios fundamentales de la seguridad informática

- 1.- Principio de menor privilegio:
  - Este es quizás el principio más fundamental de la seguridad, y no solamente de la informática. Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener tan solo los privilegios de uso necesarios para desarrollar su tarea y ninguno más.
- 2.- Seguridad no equivale a oscuridad.
  - Un sistema no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corrijamos estableciendo las medidas de seguridad adecuadas. El hecho de mantener posibles errores o vulnerabilidades en secreto no evita que existan, y de hecho evita que se corrijan.
  - No es una buena medida basar la seguridad en el hecho de que un posible atacante no conozca las vulnerabilidades de nuestro sistema. Los atacantes siempre disponen de los medios necesarios para descubrir las debilidades más insospechadas de nuestro sistema.

Principios fundamentales de la seguridad informática (II)

- 3.- Principio del eslabón más débil.
  - En un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades. Cuando diseñemos una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas. No basta con establecer unos mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.
- 4.- Defensa en profundidad.
  - La seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte que éste sea, sino que es necesario establecer varias mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

Principios fundamentales de la seguridad informática (III)

- 5.- Punto de control centralizado.
  - Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.
- 6.- Seguridad en caso de fallo.
  - Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro. Por ejemplo, si nuestros mecanismos de control de acceso al sistema fallan, es preferible que como resultado no dejen pasar a ningún usuario a que dejen pasar a cualquiera aunque no esté autorizado.

Principios fundamentales de la seguridad informática (IV)

- 7.- Participación universal.
  - La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.
- 8.- Principio de simplicidad.
  - La simplicidad es un principio de seguridad por dos razones:
    - En primer lugar, mantener las cosas simples, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro.
    - En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

Seguridad en Sistemas Operativos.

- Los sistemas Operativos (Windows, Unix, MacOs,...)son los encargados de la interacción entre los usuarios de las máquinas y los recursos informáticos.
  - Por tanto, forman la primera línea de seguridad lógica.
- Un sistema operativo “seguro” debería contemplar:
  - Identificación y autentificación de los usuarios.
  - Control de acceso a los recursos del sistema.
  - Monitorizar las acciones realizadas por los usuarios, sobre todo las que sean sensibles desde el punto de vista de seguridad.
  - Auditoría de los eventos de posible riesgo.
  - Garantía de integridad de los datos almacenados.
  - Garantía de la disponibilidad de los recursos,
  - .....

Evaluación de seguridad en Sistemas Operativos.

- Uno de los criterios de seguridad más extendido lo establece el National Computer Security Center (NCSC), publicado en 1985 como Trusted Computer Systems Evaluation Criteria (TSEC) también llamado el “libro naranja”.
  - Define 4 niveles de seguridad (D,C,B,A) con algunos subniveles:
    - D : sistema con protección mínima.
    - C1 : sistema con seguridad discrecional,
    - C2: sistema con control de accesos,
    - .....
- En la Unión Europea se publicó en 1990 el Information Technology Security Evaluation Criteria (ITSEC).
  - Define 7 niveles de seguridad algo más elaborados que los TSEC.
  - E0 : sistema con nivel de confianza nulo.
  - ....E6: Sistema con protección y diseño de máxima confianza.
- La metodologia de evaluación está definida en el ITSEM, cuya primera versión es de 1992.

Seguridad en Bases de Datos.

- La información en un sistema informático reside, fundamentalmente, en Bases de Datos cuya seguridad es, por consiguiente, de vital importancia.
- El primer filtro de seguridad de la Base de Datos lo constituye, evidentemente, el Sistema Operativo.
- No obstante, la seguridad que debe proporcionar la Base de Datos tiene algunas características diferenciadas:
  - Hay muchos más objetos a proteger.
  - El promedio de tiempo de vida de los objetos es mayor.
  - La granularidad del control es mayor.
  - Los objetos son estructuras lógicas complejas.
  - La seguridad está relacionada con la semántica de los datos, no con sus características físicas,
  - ....

Seguridad en Bases de Datos II.

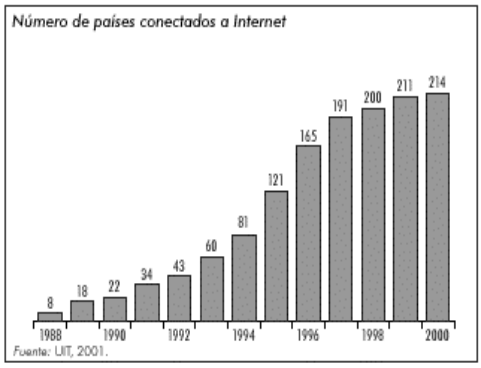
- Dada la complejidad de los problemas anteriores, es el propio Sistema de Gestión de Bases de Datos (SGBD) el que proporciona la seguridad de éstas.
- Un SGBD debe mantener los tres criterios básicos:
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.
- La seguridad en Bases de Datos se implementa mediante mecanismos de:
  - Identificación y autentificación.
  - Control de acceso a los objetos (datos y recursos).
  - Registro de auditoría.
  - Protección criptográfica de alguno de los datos.
  - ....

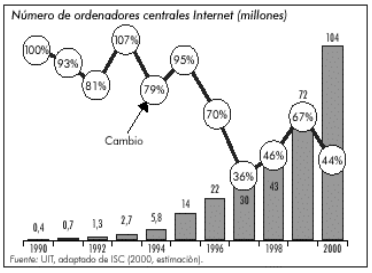
Seguridad en Bases de Datos III.

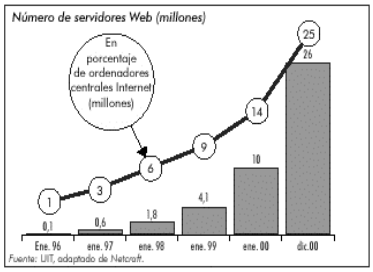
- Las posibles vulnerabilidades en la Bases de Datos son:
  - Ataques Directos: revelación, alteración y destrucción de datos.
    - La prevención frente a este tipo de ataques pasa por mecanismos de identificación, autentificación y control de acceso.
  - Ataques Directos: Inferencias estadísticas.
    - Tratan de descubrir datos sensibles, y privados, en base a parámetros estadísticos que son de acceso más libre (valores medios, desviaciones, máximos, ...)
  - Ataques indirectos: Caballo de Troya.
    - Son programas hostiles que actúan solapándose bajo un programa normal. Cuando éste se procesa, el caballo de Troya ataca a la Base de Datos soslayando los mecanismos de protección.

Seguridad en Redes.

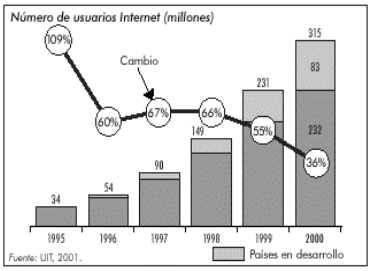
- Desde el punto de vista de seguridad una Red es “un entorno de computación con varios ordenadores independientes comunicados entre sí”.
- Las redes suponen un incremento:
  - Cuantitativo: el número de ordenadores a proteger se dispara.
  - Cualitativo: aparecen un conjunto de nuevas vulnerabilidades y amenazas.
- La “explosión” de Internet es el cambio más significativo en el mundo informático en los últimos años.
- Internet también puede considerarse como la revolución más importante en el mundo de la información desde la aparición de la imprenta.

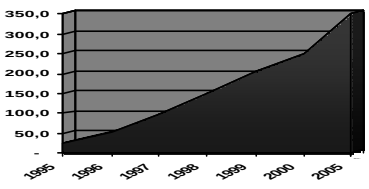






Usuarios en Internet (predicciones)





Ventajas de las redes informáticas

- Posibilidad de compartir una enorme cantidad de recursos y de información.
- Aumento de la fiabilidad y disponibilidad, debido a la redundancia.
- Posibilidad de computación distribuida.
  - El programa SETI es un ejemplo.
- Posibilidad de expansión continua de forma “transparente” (invisible) al usuario.

Desventajas de las redes informáticas

- Aumento espectacular en el número de usuarios involucrados, es decir, el número de potenciales atacantes.
- Aumento de la complejidad del sistema:
  - Distintos tipos de nodos, distintos sistemas operativos, distintas políticas de seguridad, ...
- Límites desconocidos:
  - La expansión continua de la red hace incierta la identidad de los integrantes, su situación física, los nuevos problemas que pueden surgir, etc.
- Múltiples puntos de ataque:
  - Los ataques pueden producirse tanto en los nodos origen y destino como en los dispositivos de encaminamiento, de transmisión, en los nodos intermedios, ...

Nuevas vulnerabilidades

- Privacidad:
  - Es más difícil de mantener debido a:
    - Aumento de posibles usuarios que pueden penetrar en cada nodo.
    - Aumento de los puntos en que la información puede ser interceptada.
- Integridad:
  - La transmisión de la información supone un riesgo claro.
- Autenticidad:
  - No sólo hay que identificar a los usuarios sino también a los nodos.
- Disponibilidad:
  - Es muy fácil saturar una máquina lanzando ataques desde diversos puntos de la Red.
- El mecanismo más utilizado para proporcionar seguridad en redes es la criptografía:
  - Permite establecer conexiones seguras sobre canales inseguros.

Seguridad Informática
Técnicas de Cifrado

Dr. Angel Luis Sánchez Lázaro
Profesor Titular de Universidad
Dpto. Informática y Automática
Universidad de Salamanca
<angeluis@tejo.usal.es>

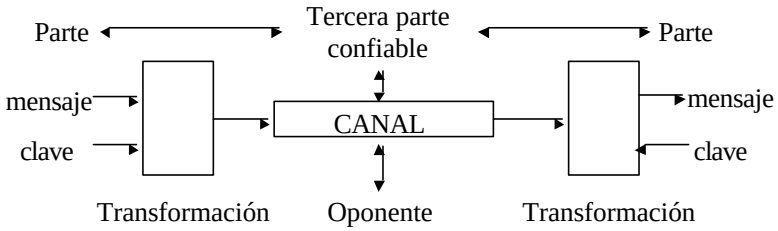
CRIPTOLOGIA

- **Criptografía**: (*Kryptos*: secreto, *Graphos*: escrito) ciencia que estudia la escritura secreta, escribir ocultando el significado.
- **Criptoanálisis:** Ciencia que estudia como hacer inteligible la escritura secreta.
- **Criptología**: Ciencia que engloba a las anteriores, criptografía y criptoanálisis.

CRIPTOANALISIS

- A partir de sólo texto cifrado.
- A partir de texto plano conocido
- Elección del mensaje
  - Texto plano elegido
  - Texto cifrado elegido
  - Texto elegido

MODELO DE SEGURIDAD



1: Algoritmo de transformación
2: Generación de información secreta
3: Distribucón y compartición de claves
4: Protocolo de intercambio para un servicio

CIFRADO

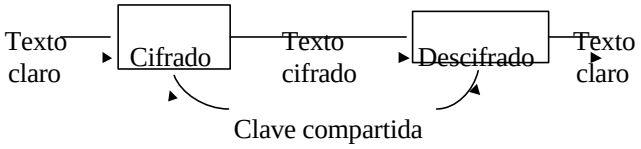
- Se asigna a cada símbolo del mensaje (letra) un código numérico
- Por una transformación se cambia el mensaje
  - Teorías de números, de información y de complejidad de algoritmos
- Tipos de transformaciones
  - Transformaciones (familias de funciones) reversibles
    - Cifrado simétrico
  - Transformaciones de una vía
    - Compendio de mensajes
  - Funciones relacionadas
    - Cifrado asimétrico

OTRAS TÉCNICAS

- Esteganografía (*Stegos*: cubierto)
  - No se trata tanto de ocultar el contenido del mensaje sino la existencia misma del mensaje.
  - Clásicamente con tinta invisible, marcado de caracteres con lapicero o agujeros con alfileres, cinta correctora de máquina
  - Equivalencia moderna scribiendo mensajes en el mismo color que el fondo, secuencias con caracteres de control que no aparezcan en pantalla (‘a’ ‘bs’ ‘b’) o fuentes distintas aunque muy parecidas.
  - Ocultar información en ficheros de imágenes o sonido.

CIFRADO SIMÉTRICO I

- Cifrado convencional, simétrico o de clave secreta
- Elementos del cifrado convencional
  - $X=\{X_1, X_2, X_3,..., X_M\}$ Texto claro
  - $K=\{K_1, K_2, K_3,..., K_J\}$ Clave
  - $Y=\{Y_1, Y_2, Y_3,..., Y_N\}$ Texto cifrado
  - L_i: letras de un alfabeto
  - $Y= E_k(X)$ $X=D_k(Y)$



CIFRADO SIMÉTRICO II

- Cifrado por sustitución monoalfabética: cada uno de los símbolos del texto claro se sustituye por otro
  - Cifrado del César: utilizado por el emperador romano

```
                0         1         2
                01234567890123456789012345
A. claro:       abcdefghijklmnopqrstuvwxyz
A. cifrado:     DEFGHIJKLMNOPQRSTUVWXYZABC
```

texto claro: nos encontramos en la plaza
texto cifrado: QRV HQFRQXUDPRV HQ OD SODCD

- $c = E(p) = (p+3) \bmod 26$ $p = D(c) = (c-3) \bmod 26$
  - Generalización: desplazamientos dependiente de clave
    - $c = E_k(p) = (p+k) \bmod 26$ $p = D_k(c) = (c-k) \bmod 26$
    - Un total de 26 funciones de cifrado distintas
  - El mensaje cifrado sigue manteniendo una estructura interna
    - Ataque por métodos estadísticos

CIFRADO SIMÉTRICO III

- Sustitución polialfabética
  - El mismo símbolo se sustituye por varios
- Ejemplo: cifrado vigenère

```
   letra clave
t. Claro   a b c d e f g h i j k l m n o p q r s t u v x y z
         a a b c d e f g h i j k l m n o p q r s t u v x y z
         b b c d e f g h i j k l m n o p q r s t u v x y z a
         c c d e f g h i j k l m n o p q r s t u v x y z a b
         d d e f g h i j k l m n o p q r s t u v x y z a b c
         e e f g h i j k l m n o p q r s t u v x y z a b c d
              ..............................
         x x y z a b c d e f g h i j k l m n o p q r s t u v
         y y z a b c d e f g h i j k l m n o p q r s t u v x
         z z a b c d e f g h i j k l m n o p q r s t u v x y
```

palabra clave: decepciondecepciondecepci
texto claro: estetextoesparaserescrito
texto cifrado: **HWVIIGFHBHWREGCASEHWEVXVW**

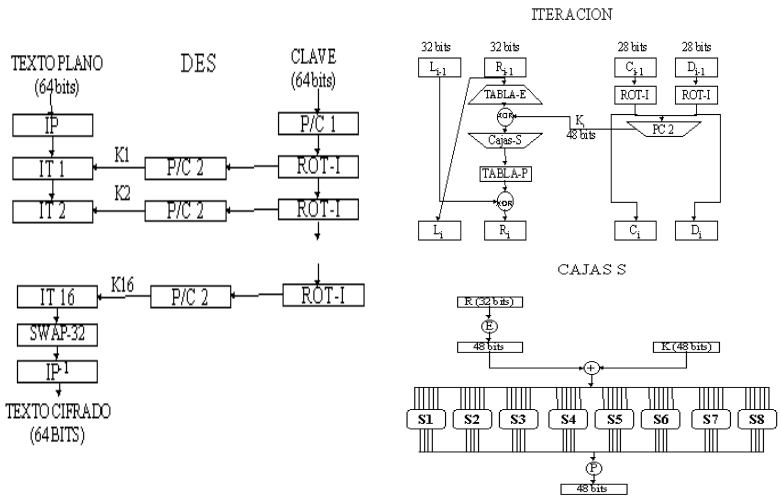
CIFRADO SIMÉTRICO IV

atencio
1735246
estetex
tosecif
rarapor
traspos
icionop

- Cifrado por trasposición o permutación
  - T. claro: este texto se cifrara por trasposicion
  - clave: atencion
  - T. Cifrado: etrti tcppn tsrai eiooo eeaso xfrsp soarc
- Algoritmos
  - DES: Data Encription Standart (clave 64 bits)
  - IDEA: International Data Encription Algorithm (128 bits)
- Problemas con las claves (una clave secreta por pareja)
  - Generación de claves
  - Administración de claves
  - Distribución de claves

DES: CIFRADO

Cifra bloques de 64 bits con una clave de 56 bits



DES: DESCIFRADO

- Mismo esquema que cifrado cambiando el orden de las subclaves

DES: MODOS DE OPERACION

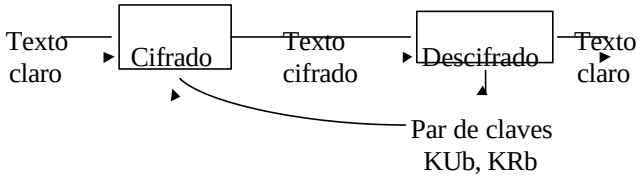
- Modo ECB: Libro de códigos. Cifrador de bloques
  $C_i = E_k(P_i)$ $P_i = D_k(C_i)$
- Modo CBC: Bloque cifrado encadenado. Cifrador de bloques
  $C_i = E_k(C_{i-1} + P_i)$ $P_i = C_{i-1} + D_k(C_i)$
- Modo CFB: Realimentación de cifrado. Cifrador de corriente
- Modo OFB: Realimentación de salida. Cifrador de corriente
- Otros modos
  - doble DES
  - triple DES
  - ampliar la longitud de la clave

OTROS ALGORITMOS DE CIFRADO SIMÉTRICO

- IDEA
  - International Data Encryption Algorithm
  - Procesa la entrada en bloques de 64 bits
  - Usa una clave de 128 bits
  - Incorpora nuevas transformaciones
    - operaciones lógicas (XOR)
    - operaciones aritméticas
      - suma y multiplicación modular
  - 9 etapas
  - 52 subclaves
  - Para descifrar se usa el mismo esquema con distintas sublaves
    - las subclaves se obtienen de las de cifrado

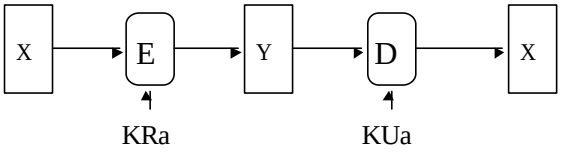
CIFRADO ASIMÉTRICO I

- Cifrado asimétrico o de clave pública
  - Un par de claves por cada entidad
  - Una para el emisor y la otra para el receptor
- Elementos del cifrado asimétrico
  - X: Texto claro
  - KU: Clave pública
  - KR: Clave privada
  - Y: Texto cifrado
  - $Y = E_{KUb}(X)$ $X = D_{KRb}(Y)$



CIFRADO ASIMÉTRICO II

- Confidencialidad con cifrado asimétrico
  - Emisor: $Y = E_{KUb}(X)$ Receptor: $X = D_{KRb}(Y)$
- Autenticación por firma con cifrado asimétrico
  - Emisor: $Y = E_{KRa}(X)$ Receptor: $X = D_{KUa}(Y)$
  - Necesidad de estructura interna del mensaje



- Confidencialidad y autenticación con cifrado asimétrico
  - Emisor: $Y = E_{KRa}(E_{KUb}(X))$ Receptor: $X = D_{KRb}(D_{KUa}(Y))$
  - Emisor: $Y = E_{KUb}(E_{KRa}(X))$ Receptor: $X = D_{KUa}(D_{KRb}(Y))$

POSTULADOS DIFFIE-HELLMAN

- Es computacionalmente fácil generar un par de claves pública y privada
- El cifrado es computacionalmente sencillo
- El descifrado, conocida la clave privada debe ser sencillo
- La obtención de la clave privada conocida la pública, es computacionalmente imposible
- Es computacionalmente imposible conocer el mensaje claro conocido el mensaje cifrado y la clave pública
- Las funciones de cifrado y descifrado pueden aplicarse en cualquier orden

ALGORITMO RSA (**R**ivest **S**hamir **A**dleman)

- Cifrado de bloques
- KU={e,n} KR={d,n}
- $C = E_{KU}(M) = M^e \bmod n$
- $M = D_{KR}(C) = C^d \bmod n = M^{ed} \bmod n$
- Generación de claves
  - Seleccionar p, q primos grandes (>150 dígitos)
  - Calcular n = pxq
  - Calcular $\phi(n) = (p-1)x(q-1)$
  - Seleccionar e $mcd(\phi(n),e) = 1$
  - Calcular $d = e^{-1} \bmod \phi(n)$

EJEMPLO DIDÁCTICO RSA

1 p = 7 q=17

2 n = pxq =7x17 = 119

3 $\phi(n) = (p-1) \times (q-1) = 96$

4 Seleccionar e primo respecto a 96 e=5

5 Calcular $d = e^{-1} \pmod{96} = 77$

KU={5,119} KR={77,119}

Cifrado M=19 M^5=2476099 $C = M^5 \bmod 119 = 66$

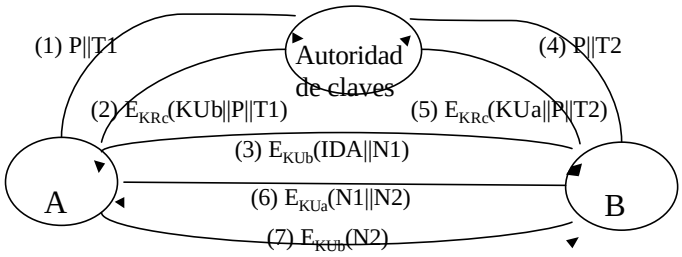
Descifrado C=66 $C^{77}=1{,}27\ 10^{40}$ $M = C^{77} \bmod 119 = 19$

INTERCAMBIO DE CLAVES PÚBLICAS I

- Anuncio público
- Directorio disponible públicamente
- Autoridad de claves públicas
- Certificado de claves públicas

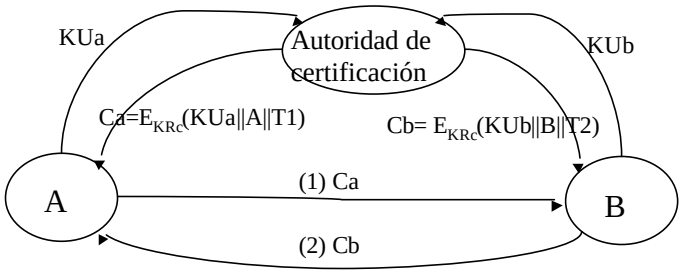
INTERCAMBIO DE CLAVES PÚBLICAS II

- Protocolo de intercambio con una autoridad de claves
  - Petición de clave de destinatario a la autoridad cada vez
  - Aumento de tráfico con la autoridad de claves



INTERCAMBIO DE CLAVES PÚBLICAS III

- Protocolo de intercambio con una autoridad de certificación (emisión de certificados)
  - Una única emisión de certificado de clave pública
  - Certifica la identidad y clave pública de una entidad
  - Se envía junto al mensaje



Servicio de autenticación

- Compendios (Funciones hash o de dispersión)
- Funciones de un sólo sentido
- Requisitos de la función H(M)
  - H puede aplicarse a mensajes de cualquier longitud
  - H produce salida de longitud fija
  - H(x) es fácil de calcular
  - Para un código dado h es infactible encontrar m, H(m)=h
  - Para un bloque dado x es infactible encontrar y, H(x)=H(y)
  - Es computacionalmente infactible encontrar x e y, H(x)=H(y)

ALGORITMO DIDACTICO

```
Sea un texto cualquiera del que se quiere
obtener su función de dispersion o funcion hash
```

Colocar el texto con un número de columnas fijo.

```
01234567
seauntex
tocualqu
ieradelq
uesequie
reobtene
rsufunci
ondedisp
ersionof
uncionha
shijklmn
zuybimbe
```

Sumar en aritmética modular por columnas el número de orden y reconvertir a símbolo

FUNCIONES HASH ESTÁNDAR

- MD5
  - Message Digest versión 5 (RFC1321)
  - Genera un código de 128 bits
  - Procesa la entrada en bloques de 512 bits
- SHA
  - Secure Hash Algorithm (FIPS PUB 180)
  - Genera un código de 160 bits
  - Procesa la entrada en bloques de 512 bits

FORMAS DE USO

- (a) A--> B $E_K(M \mid\mid H(M))$
  - Confidencialidad y Autentificación
- (b) A--> B $M \mid\mid E_K(H(M))$
  - Autentificación
- (c) A--> B $M \mid\mid E_{KRa}(H(M))$
  - Autentificación y Firma digital
- (d) A--> B $E_K(M \mid\mid E_{KRa}(H(M)))$
  - Autentificación y Firma digital. Confidencialidad
- (e) A--> B $M \mid\mid H(M \mid\mid S)$ S: valor compartido por A,B
  - Autentificación

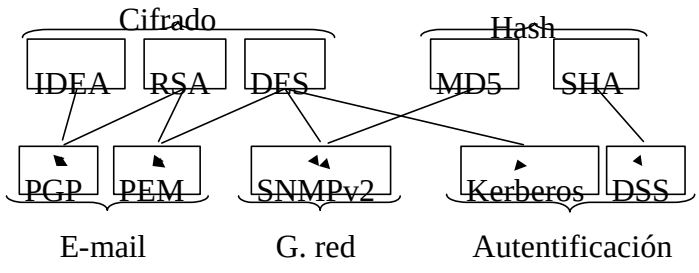
FIRMAS DIGITALES

- Propiedades:
  - Capaz de verificar autor, fecha y hora
  - Autentificar contenido a la hora de la firma
  - Verificable por terceras partes
- Requisitos:
  - Patrón de bits dependiente del mensaje que se firma
  - Información del emisor para prevenir falsificación y negación
  - Sencilla de generar
  - Sencilla de reconocer y verificar
  - Imposible de falsificar (ni firma, ni mensaje)
  - Debe ser práctico guardar una copia
- Tipos
  - Directa
  - Arbitrada

VARIAS FIRMAS

- Esquema de un mensaje con varias firmas directas y una firma arbitrada
  - Mensaje M
  - Firma 1 F1: $E_{KRx}(H(M) \,||\, T))$
  - Firma 2 F2: $E_{KRy}(H(M) \,||\, T))$
  - Firma 3 F3: $E_{KRz}(H(M) \,||\, T))$
  - Arbitro $E_{KRa}(F1 \,||\, F2 \,||\, F3 \,||\, T)$
- La firma(s) puede guardarse independientemente del mensaje

ALGORITMOS Y APLICACIONES



IDEA: **I**nternational **D**ata **E**ncryption **A**lgorithm
RSA: **R**ivest-**S**hamir-**A**dleman
DES: **D**ata **E**ncryption **S**tandard
MD5: **M**essage **D**igest v5
SHA: **S**ecure **H**ash **A**lgorithm
SNMP: **S**imple **N**etwork **M**anagement **P**.
PGP: **P**eretty **G**ood **P**rivacy
PEM: **P**rivacy **E**nhanced **M**ail
DSS: **D**igital **S**ignature **S**tandard

VISORES

CLASIFICACIÓN DE CERTIFICADOS

- Certificados son emitidos por Entidades Certificadoras
- Clasifican atendiendo a diferentes criterios:
  - **Objeto de la certificación**
    - Firma digital, intercambio de claves para confidencialidad, identidad del usuario, atributos de usuario, credenciales de pago electrónico, etc.
  - **Tipo de entidad identificada** (certificados de identidad)
    - un ciudadano, una organización, un equipo informático, una aplicación (applet), etc.
  - **Aplicación** para la que puede utilizarse el certificado. Incluye mensajería segura, servicios web, acceso remoto, etc.
  - **Nivel de garantía** del certificado.

ENTIDADES Y CLASES

- Entidades certificadoras
  - FNMT (Fabrica nacional de Moneda y Timbre)
  - Verisign
  - .....
- Clases de certificados por nivel de seguridad
  - FNMT Clase 1 CA
  - FNMT Clase 1S CA
  - FNMT Clase 2 CA

PÁGINA DEL FNMT Clase 2 CA

http://www.cert.fnmt.es/clase2/caracter.htm

CARACTERÍSTICAS

Tipo de Registro:
Presencial

Emisión del Certificado:
Claves generadas por el usuario.
Un solo par de claves sirve para firma y cifrado.
Longitud mínima sin límites. Soporte software para la clave

Gestión y uso:
Software de gestión de certificados: comercial

REQUISITOS TÉCNICOS DE USUARIO

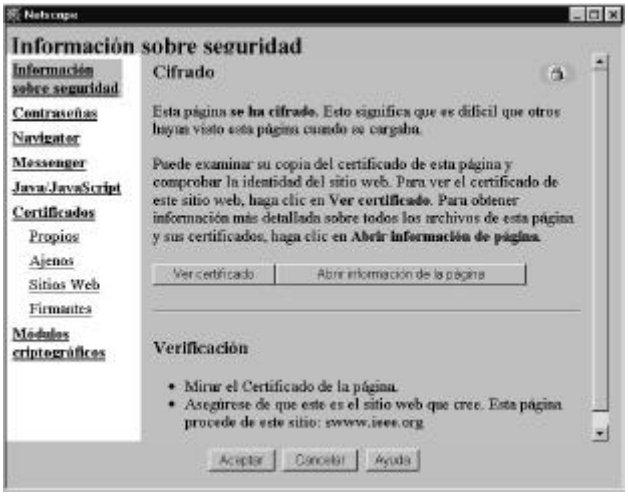
Versiones de Navegador
Las versiones de navegadores válidos para el correcto funcionamiento de este tipo de certificado son las siguientes:

Netscape
Netscape Navigator versión 4.06 o posterior, a excepción de la versión 4.60 , versiones 6.0 y posteriores, que actúe sobre un Sistema Operativo de al menos 32 bits

Microsoft
Microsoft Internet Explorer versión 4 o posterior sobre Win 32 (Windows 95 - Windows 98 - Windows NT - Windows 2000 - Windows Me).
Los usuarios de Microsoft Internet Explorer cuyo Nombre o Apellidos contengan la letra "Ñ", deberán solicitar su certificado con la Versión 5.0 de IE.

CLASE 2 CA
- CARACTERÍSTICAS Y REQUISITOS
- OBTENCIÓN DE CERTIFICADOS
- REVOCACIÓN DE CERTIFICADOS
- RENOVACIÓN DE CERTIFICADOS
- ORGANISMOS Y APLICACIONES
- COMPROBACIÓN DE DATOS
- ATENCIÓN A USUARIO

INFORMACION



CERTIFICADO

INF. CERTIFICADOS